REMARKS

Claims 1-26 are pending in the Application and are now presented for examination. Claims 1, 2, 5, 6, 10, 12, 13, 16, 17, 21 and 23-26 have been amended. No new matter has been added.

Claims 1, 10, 12, 21 and 23-26 are independent.

On page 3 of the Office Action, Claims 1-26 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,782,421, issued to Soles et al. (hereinafter "Soles) and U.S. Patent No. 6,185,589, issued to Todd Sr. et al. (hereinafter "Todd").

INDEPENDENT CLAIMS 1, 12, 23 AND 25

Independent Claims 1, 12, 23 and 25 have been amended to include the features of "detecting the presence of a security vulnerability in the system," and "responsive to detecting the presence of the security vulnerability, performing" the recited actions. Applicants assert that neither Soles nor Todd, whether standing alone or in combination, teach, disclose or suggest every element of these claims.

Regarding Claims 1, 12, 23 and 25, the Office Action characterizes Soles as teaching "the method for providing automated tracking of security vulnerabilities, comprising: using a computer device to perform a security vulnerability assessment on a system, storing data obtained from the security vulnerability assessment in a security vulnerabilities database, determining using a computer, a security vulnerability score based on a plurality of vulnerability factors identified by the vulnerability assessment" (internal citations omitted). The Office Action relies upon Todd to teach the additional feature "determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the

determined security vulnerability score." Applicants respectfully disagree with the characterization of Soles and Todd and reasserts that Soles and Todd, either standing alone or in combination, do not teach or suggest the features of Claims 1, 12, 23 and 25.

Soles teaches a method for evaluating the performance of a computer-implemented application based on the *availability* of the application—not a method for automatically tracking security vulnerabilities of the entire computer system. The word "security" appears in only two instances in Soles. The first instance, as cited in the office Action, occurs in the Background Section in a discussion of the general role of a service level agreement (SLA) between a network service provider and a customer. An SLA is defined as "a contract between a service provider and a customer that specifies measurable service parameters and outlines penalties to be imposed against the provider should the service level fall short of the agreed terms." *See* Soles, col. 1, lines 32-37. Specifically, the Office Action cites, "[t]o ensure consistent end-to-end performance, SLAs often include basic areas of operations and management such as backup schedules, software updates, systems monitoring, and maintenance, and even security." Soles, col. 2, lines 3-7. There is no mention of using the methods disclosed in Soles "to perform a security vulnerability assessment on a system."

The second occurrence of the word "security" is in connection with a "vulnerabilities survey data module." *See* Soles, col. 8, line 55 – col. 9, line 13. The vulnerabilities survey data module contains "information collected from a *survey* distributed to a diverse group of individuals having cognizance of various aspects of the application and the associated system architecture," wherein the survey may includes questions relating to such areas as "internal and external service agreements, architecture, application performance, systems/network

management, processes and procedures, business continuity/disaster recovery, and security." *See id* (emphasis added). There is no other mention of "security" throughout the entirety of Soles. Soles does not disclose actually **performing** "a security vulnerability assessment on a system," nor does it disclose "detecting the presence of a security vulnerability in the system." Soles merely discloses using information obtained from questioning users of the system about their opinions regarding the general performance of the system and using the results of those survey questions as a basis for determining system or application performance.

Soles certainly does not disclose, teach or suggest actually *performing* a security vulnerability assessment and further acting only upon the *detection* of a security vulnerability within the system.

Additionally, a "vulnerability," as discussed by Soles, concerns "evaluating business risk associated with the implementation and operation of an application" based upon the answers to survey questions received from users. In contrast, the present invention concerns actual discovery and tracking of potential security issues present within a computer system.

Applicants further respectfully disagree with the Office Action's characterization of Todd. Todd does not disclose "determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score." Rather, Todd merely discloses that a report file and results of a security assessment are only kept for a predetermined amount of time in order to "minimize the potential that another party may obtain access to the security assessment report." *See* Todd, col. 7, lines 1-8. Todd does not teach, disclose or suggest determining a time to actually ***fix*** the security vulnerability detected by the assessment based upon the security vulnerability score. Todd does not tie any

timeframe to fix vulnerabilities to a certain score. Thus, the Office Action's characterization of Todd is unsupported by the art. The Office Action notes that Soles does not teach this feature (page 4, lines 3-5).

In contract to Claims 1, 12, 23 and 25, the cited references do not teach, disclose or suggest "detecting the presence of a security vulnerability in the system," performing actions "responsive to detecting the presence of the security vulnerability," and "determining a time to fix the security vulnerability detected by the assessment based upon the security vulnerability score." For at least these reasons, Applicants believe Claims 1, 12, 23 and 25, as amended, are sufficient to overcome the rejection under 35 U.S.C. § 103(a). The withdrawal of this rejection is earnestly solicited.

INDEPENDENT CLAIMS 10, 21, 24 AND 26

Independent Claims 10, 21, 24 and 26, have herein been amended to clearly recite A feature whereby the security vulnerabilities are "detected in the computer system" (emphasis added). Additionally, Claims 10, 21, 24 and 26 have been amended to recite "measuring a frequency of occurrence for the detected security vulnerabilities" (emphasis added). Measuring a frequency of occurrence requires the frequency of occurrence to be based upon quantifiable data. These features are not taught, disclosed, or suggested by Soles or Todd, whether considered alone or in combination.

The Office Action characterizes Soles as disclosing "a method for determining a criticality factor for a security vulnerability in a computer system, comprising: Entering in a database security vulnerabilities identified during a security vulnerability assessment. Monitoring a frequency of occurrence for the identified security vulnerabilities. Assigning a

security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system" (internal citations omitted).

As discussed above in relation to Claims 1, 12, 23 and 25, Soles does not disclose "entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment" (emphasis added). Soles does not teach, disclose or suggest actually performing a security vulnerability assessment on the computer system and entering those security vulnerabilities actually detected during the assessment in a database.

Moreover, Soles does not teach or suggest the feature of "measuring a frequency of occurrence for the detected security vulnerabilities" as recited in independent Claims 10, 21, 24 and 26. In contrast, Soles discloses including frequency of occurrence questions in the vulnerability survey to poll survey respondents as to their perception of "how often the best practice occurs or how often it *should* occur." *See* Soles, col. 9, lines 35-39 (emphasis added). According to Soles, the "frequency" is assessed on a scale of 0-5, with 0 being "will not occur" and 5 being "frequent – likely to occur on a regular basis, more frequently than once a quarter." *See* Soles, FIG. 16. Soles does not disclose actually measuring the frequency that a security vulnerability occurs based upon quantifiable detection of the vulnerability in the computer system.

In contrast to Claims 10, 21, 24 and 26, the cited references do not teach, disclose or suggest "entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment" and "measuring a frequency of occurrence for the detected security vulnerabilities" (emphasis added). For at least this reason, Applicants believe Claims

10, 21, 24 and 26, as amended, are sufficient to overcome the rejection under 35 U.S.C. § 103(a). The withdrawal of this rejection is respectfully requested.

DEPENDENT CLAIMS 6 AND 17

Regarding Claims 6 and 17, the Office Action characterizes Soles as teaching "determining delinquent security vulnerabilities based upon the determined time to fix the vulnerability identified by the security vulnerability assessment." Applicants respectfully disagree with this characterization. The Office Action cites to a passage wherein a grade for *applications* which do not meet service target levels is lowered. *See* Soles, col. 7, lines 1-7. This passage does not disclose rendering certain security vulnerabilities delinquent based upon the time determined for the vulnerability to be fixed. The grade in Soles relates to meeting specified service level goals by an application. If the application fails to meet some of these goals, but not all of the goals, the grade is affected accordingly. However, as recited in the Claims 6 and 17, the present invention identifies specific security vulnerabilities present on a computer system. Each security vulnerability is assigned a score based upon a number of factors. This score is then used to set a timeframe for fixing (i.e. eliminating) the vulnerability. The set timeframe does not change; thus, once the time has passed for fixing the problem and the vulnerability still exists, it is then delinquent. There is no scaled grade to be affected—the mere continued presence of the vulnerability beyond the time determined to eliminate the vulnerability means that the vulnerability is delinquent. This feature is not disclosed, taught, or suggested by Soles or Todd; thus, Applicants respectfully request withdrawal of the 35 USC § 103(a) rejection.

DEPENEDNT CLAIMS 2-9, 11, 13-20 AND 22

Claims 2-9, 11, 13-20 and 22 are each dependent either directly or indirectly from one or another of independent Claims 1, 10, 12 and 21 discussed above. These claims recite additional limitations which, in conformity with the features of their corresponding independent claim, are not disclosed or suggested by the art of record. The dependent claims are therefore believed patentable. However, the individual reconsideration of the patentability of each claim on it own merits is respectfully requested.

For all of the above reasons, the claim objections are believed to have been overcome placing Claims 1-26 in condition for allowance, and reconsideration and allowance thereof is respectfully requested.

The Examiner is encouraged to telephone the undersigned to discuss any matter that would expedite allowance of the present application. The Commissioner is hereby authorized to credit overpayments or charge payment of any additional fees associated with this communication to Deposit Account No. 090457.

Respectfully submitted,

Date: January 3, 2008

By: /Alan M. Weisberg/

Alan M. Weisberg
Reg. No.: 43,982
Attorney for Applicant(s)
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No. 68786
Tel: (954) 828-1488
Fax: (954) 828-9122
email: ptomail@cwiplaw.com

94229